Desktop Firewall Rules

Roll No: 1942

1. Check firewall status

   Systemctl status|start|stop|restart firewalld

```
[root@fedora nehalparsekar]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2021-09-19 14:35:53 IST; 9min ago
       Docs: man:firewalld(1)
   Main PID: 741 (firewalld)
      Tasks: 2 (limit: 4653)
     Memory: 47.4M
        CPU: 937ms
     CGroup: /system.slice/firewalld.service
             └─741 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Sep 19 14:35:52 fedora systemd[1]: Starting firewalld - dynamic firewall daemon...
Sep 19 14:35:53 fedora systemd[1]: Started firewalld - dynamic firewall daemon.
[root@fedora nehalparsekar]#
```

2. List Firewall chains and their rules (default table = filter)

   iptables -L

```
[root@fedora nehalparsekar]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@fedora nehalparsekar]#
```

3. List specific chain(default table = filter)

   iptables -L INPUT

```
[root@fedora nehalparsekar]# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
[root@fedora nehalparsekar]#
```

4. List specific chain from specific table (filter table)

   iptables -t filter -L INPUT

```
[root@fedora nehalparsekar]# iptables -t filter -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
[root@fedora nehalparsekar]#
```

5. Backup old rules

   Iptables-save > filename

```
[root@fedora nehalparsekar]# iptables-save > firewallRulesBackup
[root@fedora nehalparsekar]#
```

6. Restore old rules

   Iptables-restore filename

```
[root@fedora nehalparsekar]# iptables-restore firewallRulesBackup
[root@fedora nehalparsekar]#
```

7. Flush all rules from “filter” tables

```
[root@fedora nehalparsekar]# iptables -F
[root@fedora nehalparsekar]# iptables -t filter -F
```

8. Flush chains and the rules from “filter” table

```
[root@fedora nehalparsekar]# iptables -X
[root@fedora nehalparsekar]# iptables -t filter -X
[root@fedora nehalparsekar]#
```

9. Set default policy to drop on all chains in filter table

```
[root@fedora nehalparsekar]# iptables -P INPUT DROP
[root@fedora nehalparsekar]# iptables -P OUTPUT DROP
[root@fedora nehalparsekar]# iptables -P FORWARD DROP
[root@fedora nehalparsekar]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
[root@fedora nehalparsekar]#
```

10. Allow all packages to go out

```
[root@fedora nehalparsekar]# iptables -A OUTPUT -j ACCEPT
[root@fedora nehalparsekar]# iptables -L OUTPUT
Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
[root@fedora nehalparsekar]#
```

11. Allow input packets if they are related to the output

```
[root@fedora nehalparsekar]# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
[root@fedora nehalparsekar]# iptables -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
[root@fedora nehalparsekar]#
```

12. Delete a rule

```
[root@fedora nehalparsekar]# iptables -D OUTPUT -j ACCEPT
[root@fedora nehalparsekar]#
```

13. Allow output to be only TCP traffic

```
[root@fedora nehalparsekar]# iptables -A OUTPUT -p tcp -j ACCEPT
[root@fedora nehalparsekar]# iptables -t filter  -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
[root@fedora nehalparsekar]#
```

14. Allow UPD traffic output

```
[root@fedora nehalparsekar]# iptables -A OUTPUT -p udp -j ACCEPT
[root@fedora nehalparsekar]# iptables -t filter -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             anywhere
[root@fedora nehalparsekar]#
```

15. Allow UDP packets only on DNS PORT(53)

```
[root@fedora nehalparsekar]# iptables -A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
[root@fedora nehalparsekar]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
[root@fedora nehalparsekar]#
```

16. Allow tcp traffic to be only http(80) and https(443)

```
[root@fedora nehalparsekar]# iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
[root@fedora nehalparsekar]# iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
[root@fedora nehalparsekar]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
[root@fedora nehalparsekar]#
```

17. Allow ICMP traffic for ping

```
[root@fedora nehalparsekar]# iptables -A OUTPUT -p icmp -m icmp --icmp-type echo-request -j ACCEPT
[root@fedora nehalparsekar]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
[root@fedora nehalparsekar]#
```